Journal of Pure and Applied Algebra 55 (1988) 199–211
North-Holland

SELF-DUAL GOPPA CODES

Henning STICHTENOTH
Fachbereich 6 – Mathematik, Universität-Gesamthochschule Essen, D4300 Essen 1, Fed. Rep. Germany

Communicated by F. Oort
Received 15 December 1986
Revised 18 June 1987

For an algebraic function field $F/\mathbb{F}_q$ and two divisors G and D of F (where $D = P_1 + \cdots + P_n$ and $\deg(P_i) = 1$) Goppa constructed a code C over $\mathbb{F}_q$. In the present paper sufficient conditions for self-duality resp. self-orthogonality of C are given in terms of the divisors G and D. Several examples are presented.

0. Introduction

Goppa showed in his fundamental paper [8] how to construct linear codes by means of algebraic curves over a finite field $\mathbb{F}_q$. The main parameters of these codes (length, dimension, minimum distance) may easily be interpreted, because they have a simple geometric meaning. These codes, which are called 'geometric Goppa codes', contain the class of 'classical Goppa codes' [12, 13], which were introduced by Goppa in 1970. So far, the most interesting application of geometric Goppa codes seems to be the construction of families of long codes that are asymptotically better than the Gilbert–Varshamov bound [10, 14, 17].

In several papers [4, 5, 6] Driencourt and Michon investigated certain geometric Goppa codes which are defined by elliptic curves over a field of characteristic 2. One of their main results is concerned with the question whether these codes are self-dual. The aim of our paper is to prove a much more general criterion for self-duality of geometric Goppa codes (see Section 3 below). This criterion contains the criterion of Driencourt and Michon, and it holds for curves of arbitrary genus over any finite field.

In Section 1 we introduce the notations used in this paper; Section 2 contains the definition and elementary properties of geometric Goppa codes. Usually one describes these codes in the language of algebraic curves [8, 15], but here we use the language of algebraic function fields of one variable [2, 3]. The main part of our paper is Section 3, where we state some criteria for self-duality resp. self-orthogonality of geometric Goppa codes. Finally, in Section 4, we obtain some classes of examples to demonstrate the range of our results.

1. Notations

General references for the algebraic-geometrical background are [2] and [3]; for coding theory see [12] and [13]. Let

- $\mathbb{F}_q$ the finite field with q elements,
- $\mathbb{F}_q^\times$ the group of units of $\mathbb{F}_q$,
- F a field of algebraic functions of one variable over $\mathbb{F}_q$, such that $\mathbb{F}_q$ is algebraically closed in F,
- g the genus of F,
- Ω the module of differentials of F over $\mathbb{F}_q$,
- $(x)_0$ the zero divisor of $0 \neq x \in F$,
- $(x)_\infty$ the pole divisor of $0 \neq x \in F$,
- (x) the principal divisor of $0 \neq x \in F$, i.e. $(x) = (x)_0 - (x)_\infty$,
- (η) the divisor of a differential $0 \neq \eta \in \Omega$,
- v_P the valuation of F, which belongs to a place P of $F/\mathbb{F}_q$, written additively.

For a place P of degree one, an element $x \in F$ with $v_P(x) \geq 0$ and a differential $\eta \in \Omega$ let

$x(P)$ the value of x at P (i.e. $x(P) \in \mathbb{F}_q$ and $v_P(x - x(P)) > 0$),
$\operatorname{res}_P(\eta)$ the residue of η at P.

The divisor group of F is written additively. For a divisor A we have

- $L(A) = \{x \in F \mid (x) \geq -A\}$,
- $\Omega(A) = \{\omega \in \Omega \mid (\omega) \geq A\}$,
- $\dim(A)$ the dimension of $L(A)$ over $\mathbb{F}_q$,
- $i(A)$ the dimension of $\Omega(A)$ over $\mathbb{F}_q$.

The Riemann–Roch theorem states that

$$\dim(A) = \deg(A) + 1 - g + i(A) \quad \text{and} \quad i(A) = \dim(W - A),$$

where W is an arbitrary canonical divisor of F (i.e. $W = (\omega)$ with $0 \neq \omega \in \Omega$).

Two divisors A, B are called equivalent, if there is an $x \in F$ with $A = B + (x)$.

Throughout the whole paper, we fix the following situation:

- $P_1, \ldots, P_n$ are pairwise different places of $F/\mathbb{F}_q$ of degree one,
- $D = P_1 + \cdots + P_n$,
- G is a divisor of F with $v_{P_i}(G) = 0$ $(i = 1, \ldots, n)$.

It is not necessary that G is positive (as it is always assumed in [8, 11, 15]).

A linear code of length n over $\mathbb{F}_q$ is a linear subspace of $\mathbb{F}_q^n$. There is a canonical non-degenerate bilinear form on $\mathbb{F}_q^n \times \mathbb{F}_q^n$, defined by

$$\langle (a_1, \ldots, a_n), (b_1, \ldots, b_n) \rangle = a_1 b_1 + \cdots + a_n b_n.$$

For a linear code C of length n, the code

$$C^{\perp} = \{x \in \mathbb{F}_q^n \mid \langle x, z\rangle = 0 \text{ for any } z \in C\}$$

is called its dual code. $C^{\perp}$ is linear, and we have

$$\dim(C) + \dim(C^{\perp}) = n.$$

C is called self-dual if $C = C^{\perp}$; it is called self-orthogonal (or weakly self-dual, cf. [13]), if $C \subseteq C^{\perp}$. The weight $w(z)$ of a vector $z \in \mathbb{F}_q^n$ is the number of its nonzero coordinates; the minimum distance $d(C)$ of a linear code $C \neq 0$ is defined by

$$d(C) = \min\{w(z) \mid 0 \neq z \in C\}.$$

An $[n, k, d]$-code is a linear code of length n, dimension k and minimum distance d.

2. Geometric Goppa codes

In this chapter we shall define the geometric Goppa codes by means of an algebraic function field $F/\mathbb{F}_q$ and two divisors G, D of F (observe the assumptions on G and D in Section 1).

Definition. $C(G, D) := \{(x(P_1), \ldots, x(P_n)) \mid x \in L(G)\}$.

Evidently, $C(G, D)$ is a linear code of length n over $\mathbb{F}_q$.

Lemma 2.1. *$C(G, D)$ is an $[n, k, d]$-code with*

$$k = \dim(G) - \dim(G - D).$$

If $k > 0$, then we have

$$d \geq \deg(D - G).$$

Proof. Consider the surjective linear map $\varphi : L(G) \to C(G, D)$ with $\varphi(x) := (x(P_1), \ldots, x(P_n))$. The kernel of φ is $L(G - D)$, so $\dim(C(G, D)) = \dim(G) - \dim(G - D)$. Assume now that $k > 0$. Let $d = d(C(G, D))$ and $x \in L(G)$ such that $w(\varphi(x)) = d$. Then there are exactly $n - d$ places $P_{i_1}, \ldots, P_{i_{n-d}}$ in the support of D which are zeroes of x, and so

$$0 \neq x \in L(G - (P_{i_1} + \cdots + P_{i_{n-d}})).$$

We conclude

$$0 \leq \deg(G - (P_{i_1} + \cdots + P_{i_{n-d}})) = \mathrm{d} - \deg(D - G). \qquad \square$$

Remark 2.2. Let $\dim(C(G, D)) > 0$ and $\delta := \deg(D - G) > 0$. Assume there is a positive divisor $D' \leq D$ with the following properties:

$$\deg(D') = n - \delta \quad \text{and} \quad \dim(G - D') > 0.$$

Then $C(G, D)$ has minimum distance $d = \deg(D - G)$.

Proof. Choose $0 \neq x \in L(G - D')$. Since $\deg(G - D') = \deg(G) - n + \delta = 0$, we have $(x) = D' - G$. It follows that the codeword $(x(P_1), \ldots, x(P_n)) \in C(G, D)$ has weight δ. □

Definition. $C^*(G, D) := \{(\operatorname{res}_{P_1} \omega, \ldots, \operatorname{res}_{P_n} \omega) \mid \omega \in \Omega(G - D)\}$.

The codes $C(G, D)$ and $C^*(G, D)$ are called the *geometric Goppa codes* with respect to G and D.

Lemma 2.3. *$C^*(G, D)$ is an $[n, k^*, d^*]$-code with*

$$k^* = i(G - D) - i(G).$$

If $k^* > 0$, then we have

$$d^* \geq \deg(G) - 2g + 2. \qquad \square$$

We omit the proof of Lemma 2.3; it is similar to Lemma 2.1.

Theorem 2.4. (Goppa [8]).

$$C(G, D)^{\perp} = C^*(G, D).$$

Proof. Let $x \in L(G)$, $\omega \in \Omega(G - D)$. Then

$$\langle (x(P_1), \ldots, x(P_n)), (\operatorname{res}_{P_1} \omega, \ldots, \operatorname{res}_{P_n} \omega) \rangle$$
$$= \sum_{i=1}^{n} x(P_i) \cdot \operatorname{res}_{P_i} \omega = \sum_{i=1}^{n} \operatorname{res}_{P_i}(x\omega) = 0.$$

(The last equation holds by the residue formula; one has to observe that the only poles of $x\omega$ are in the support of D.) Hence, $C^*(G, D) \subset C(G, D)^{\perp}$. From Lemmas 2.1 and 2.3 and the Riemann-Roch theorem we have

$$\dim(C(G, D)) + \dim(C^*(G, D)) = n,$$

so we conclude $C^*(G, D) = C(G, D)^{\perp}$. □

Definition. Let $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q^{\times})^n$ and $C \subseteq \mathbb{F}_q^n$. Then

$$a \cdot C := \{(a_1 x_1, \ldots, a_n x_n) \mid (x_1, \ldots, x_n) \in C\}.$$

Obviously, $a \cdot C$ is a linear code iff C is a linear code. These codes have the same dimension, the same minimum distance and the same weight distribution.

Theorem 2.5. *Assume W is a canonical divisor of F with $v_{P_i}(W) = -1$ $(i = 1, \ldots, n)$.*

Let $H := D - G + W$. *Then we have* $v_{P_i}(H) = 0$ $(i = 1, \ldots, n)$, *and there is an* $a \in (\mathbb{F}_q^{\times})^n$ *such that*

$$C^*(G, D) = a \cdot C(H, D).$$

One can determine a *as follows: Choose a differential* $\eta \in \Omega$ *with* $(\eta) = W$ *and take* $a := (\mathrm{res}_{P_1} \eta, \ldots, \mathrm{res}_{P_n} \eta)$.

Proof. Consider the following commutative diagram:

$$\begin{array}{ccc} L(H) & \xrightarrow{f} & \Omega(G-D) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \psi} \\ C(H,D) & \xrightarrow{h} & C^*(G,D) \end{array}$$

The mappings in this diagram are defined as follows:

$$f(x) := x\eta,$$

$$\varphi(x) := (x(P_1), \ldots, x(P_n)),$$

$$\psi(\omega) := (\mathrm{res}_{P_1} \omega, \ldots, \mathrm{res}_{P_n} \omega),$$

$$h(u_1, \ldots, u_n) := (u_1 \cdot \mathrm{res}_{P_1} \eta, \ldots, u_n \cdot \mathrm{res}_{P_n} \eta).$$

Observe that f is an isomorphism (by the Riemann–Roch theorem) and φ, ψ are surjective. So h is surjective. Evidently, h is injective, hence an isomorphism. This means $C^*(G, D) = a \cdot C(H, D)$. □

Corollary 2.6. *One can find a canonical divisor* W *with the following properties*:

$$v_{P_i}(W) = -1 \quad (i = 1, \ldots, n), \quad \text{and} \quad C^*(G, D) = C(D - G + W, D).$$

Proof. The theorem of independence [3] assures that there is a differential $\eta \in \Omega$ with $v_{P_i}(\eta) = -1$ and $\mathrm{res}_{P_i}(\eta) = 1$ for $i = 1, \ldots, n$. Take $W := (\eta)$. □

Corollary 2.7. *Let* η, H, a *be as in Theorem* 2.5. *Then*

$$C(G, D)^{\perp} = a \cdot C(H, D). \qquad \square$$

3. Self-orthogonal and self-dual geometric Goppa codes

The results of Section 2 give a very simple sufficient criterion for self-orthogonality resp. self-duality of geometric Goppa codes.

Theorem 3.1. *Assume there is a canonical divisor W with the properties*

$$(1)\ W \geq 2G - D \quad \text{and} \quad (2)\ v_{P_i}(W) = -1 \quad (i = 1, \ldots, n).$$

Then there is an $a \in (\mathbb{F}_q^\times)^n$ such that

$$a \cdot C(G, D) \subseteq C(G, D)^\perp.$$

One can determine a as follows: Choose $\eta \in \Omega$ with $(\eta) = W$ and take $a := (\mathrm{res}_{P_1} \eta, \ldots, \mathrm{res}_{P_n} \eta)$.

Supplement to Theorem 3.1. *If one replaces condition* (1) *in Theorem* 3.1 *by the stronger condition* (1′) $W = 2G - D$, *then*

$$a \cdot C(G, D) = C(G, D)^\perp.$$

Proof of Theorem 3.1. From the assumption (1) we have

$$G \leq W + D - G =: H.$$

Hence $L(G) \subseteq L(H)$ and $C(G, D) \subseteq C(H, D)$. By Corollary 2.7

$$a \cdot C(G, D) \subseteq a \cdot C(H, D) = C(G, D)^\perp.$$

The supplement is trivial. □

Corollary 3.2. *Assume there is a differential $\eta \in \Omega$ with the following properties:*

$$(1)\ (\eta) \geq 2G - D \quad \text{and} \quad (2)\ \mathrm{res}_{P_i} \eta = \mathrm{res}_{P_j} \eta \neq 0 \quad \text{for } 1 \leq i, j \leq n.$$

Then $C(G, D)$ is self-orthogonal. □

Corollary 3.3. *Assume there is a differential $\eta \in \Omega$ with the following properties:*

$$(1)\ (\eta) = 2G - D \quad \text{and} \quad (2)\ \mathrm{res}_{P_i} \eta = -\mathrm{res}_{P_j} \eta \quad \text{for } 1 \leq i, j \leq n.$$

Then $C(G, D)$ is a self-dual $[n, \frac{1}{2}n, d]$-code with $d \geq \frac{1}{2}n + 1 - g$. □

These corollaries are immediate consequences of Theorem 3.1 and Lemma 2.1. Observe that the codes considered in Corollary 3.3 have a rather large minimum distance if g is small with respect to n.

Corollary 3.4. *Assume there is a differential $\eta \in \Omega$ with the following properties:*
(1) $(\eta) \geq 2G - D$ *and*
(2) *For $i = 1, \ldots, n$ there is an element $b_i \in \mathbb{F}_q^\times$ with $\mathrm{res}_{P_i} \eta = b_i^2$.*
Then there exists a divisor G' equivalent to G such that $C(G', D)$ is self-orthogonal.

Supplement 1 to Corollary 3.4. *If we replace condition* (1) *in Corollary* 3.4 *by the stronger condition* (1′) $(\eta) = 2G - D$, *then the code $C(G', D)$ is self-dual.*

Supplement 2 to Corollary 3.4. *If q is a power of 2, condition* (2) *in Corollary* 3.4 *is always valid.*

Proof. Choose $u \in F$ with $v_{P_i}(u) = 0$ and $u(P_i) = b_i$ $(i = 1, \ldots, n)$. This is possible by the theorem of independence. Let $G' := G - (u)$. Then

$$2G' - D = 2G - D + (u^{-2}) \leq (u^{-2}\eta).$$

Since

$$\operatorname{res}_{P_i}(u^{-2}\eta) = b_i^{-2} \operatorname{res}_{P_i} \eta = 1,$$

$C(G', D)$ is self-orthogonal by Corollary 3.2. Supplement 1 is trivial; Supplement 2 follows from the fact that the Frobenius map $c \to c^2$ is an automorphism of $\mathbb{F}_q$ if q is a power of 2. □

Remark 3.5. In the very special case $g = 1$, $q = 2^e$, Corollary 3.3 was announced by Driencourt and Michon for particular divisors G and D [4, p. 17].

Before giving some explicit examples we want to point out the meaning of Theorem 3.1 in the case of the rational function field $F = \mathbb{F}_q(x)$, i.e. $g = 0$.

Corollary 3.6. *If $g = 0$, then the following assertions are equivalent:*
(1) $\deg(G) = \frac{1}{2}n - 1$.
(2) *There is an $a \in (\mathbb{F}_q^{\times})^n$ with $C(G, D)^{\perp} = a \cdot C(G, D)$.*

Proof. This is an immediate consequence of the Riemann–Roch theorem; one has to observe that every divisor of degree -2 is canonical. □

Corollary 3.7. *Let $g = 0$ and $q \equiv 0 \equiv 0 \bmod 2$. Then there is a divisor G of degree $\frac{1}{2}n - 1$ such that $C(G, D)$ is a self-dual $[n, \frac{1}{2}n, \frac{1}{2}n + 1]$-code.*

Proof. This follows from Corollary 3.6 and Supplement 2 to Corollary 3.4. Observe that the minimum distance d of an $[n, \frac{1}{2}n]$-code cannot exceed $\frac{1}{2}n + 1$ (singleton bound for codes [13]), so we obtain $d = \frac{1}{2}n + 1$ from Corollary 3.3. □

Remark 3.8. The codes in Corollary 3.7 are MDS codes (maximum distance separable codes [13]). Their length is bounded by q since $\mathbb{F}_q(x)$ has exactly $q + 1$ places of degree one.

4. Examples

Of course, the preceding results are of significance only if there are interesting examples of function fields $F/\mathbb{F}_q$ and divisors G, D with the properties assumed in

Theorem 3.1. Hence, in this chapter we describe three general examples where the assumptions of Theorem 3.1 are fulfilled (actually, Example 4.1 is a special case of Example 4.3, but for the convenience of the reader it may be helpful to treat this case separately). We shall not prove all details in our examples; for this we refer to [9].

Example 4.1 (Some 'hyperelliptic' codes in characteristic 2).

Let $q=2^e$ and $F=\mathbb{F}_q(x,y)$ be defined by the equation

$$y^2+y=f(x), \qquad f(x)\in\mathbb{F}_q[x], \qquad \deg f=:m\not\equiv 0 \bmod 2.$$

This function field has genus $g=\frac{1}{2}(m-1)$ (see [16]); it is elliptic in case $m=3$, and for $m\geq 5$ it is hyperelliptic. The pole of x is ramified in the field extension $F/\mathbb{F}_q(x)$, i.e. $(x)_\infty=2P_\infty$ with a place P_∞ of degree one. Let

$$M:=\{\alpha\in\mathbb{F}_q \mid \text{there is } \beta\in\mathbb{F}_q \text{ such that } \beta^2+\beta=f(\alpha)\}.$$

For $\alpha\in M$ the zero divisor of $x+\alpha$ takes the form

$$(x+\alpha)_0=P_1^{(\alpha)}+P_2^{(\alpha)}, \qquad P_1^{(\alpha)}\neq P_2^{(\alpha)}, \qquad \deg(P_1^{(\alpha)})=\deg(P_2^{(\alpha)})=1.$$

In this way all places of $F/\mathbb{F}_q$ of degree one (except P_∞) are obtained. Now let

$$U\subseteq M, \qquad |U|=:s>0, \qquad n=2s,$$

$$\varphi(x):=\prod_{\alpha\in U}(x+\alpha) \quad \text{and} \quad D:=(\varphi(x))_0.$$

We have

$$D=P_1+\cdots+P_n$$

with pairwise different places P_i of degree one. Define

$$G:=r\cdot P_\infty \quad \text{with } r:=\frac{m-3}{2}+s, \quad \text{and} \quad \eta:=\frac{dx}{\varphi(x)}.$$

Then $2G-D=(\eta)$. By Theorem 3.1 we conclude

$$C(G,D)^\perp=a\cdot C(G,D) \quad \text{with } a=(\mathrm{res}_{P_1}\eta,\ldots,\mathrm{res}_{P_n}\eta).$$

For a suitable divisor G' equivalent to G we find a self-dual code $C(G',D)$ of length $n=2s$ (see Supplement 2 to Corollary 3.4).

The question whether one can construct long self-dual codes in this manner is of particular interest. The length of the codes in Example 1 is bounded by

$$n\leq q+2gq^{1/2}=q+(m-1)q^{1/2}.$$

(This is the classical Hasse-Weil inequality, cf. [1]). For suitable polynomials $f(x)$ this bound is attained as the following example shows:

Example 4.1.1. Consider (in Example 4.1) the particular case

$$q = Q^2 \quad \text{with } Q = 2^h \quad \text{and} \quad F = \mathbb{F}_q(x, y) \quad \text{with } y^2 + y = x^{Q+1}.$$

In this case all places of $\mathbb{F}_q(x)$ of degree 1 except the pole of x are decomposed in the extension $F/\mathbb{F}_q(x)$, hence F has exactly

$$1 + 2q = 1 + q + 2gq^{1/2}$$

places of degree one. Choose

$$D := (x^q + x)_0 \quad \text{and} \quad G := \left(q - 1 + \frac{Q}{2}\right) \cdot P_\infty.$$

The differential

$$\eta := \frac{\mathrm{d}x}{x^q + x}$$

has the properties

$$(\eta) = 2G - D \quad \text{and} \quad \operatorname{res}_P \eta = 1$$

for any place P in the support of D. We conclude that $C(G, D)$ is a self-dual $[2q, q, d]$-code over $\mathbb{F}_q$ with minimum distance $d \geq q + 1 - \frac{1}{2}Q$.

Example 4.1.2. This example shows that the code $C(G, D)$ may be self-dual also in the case where $2G - D$ is not canonical. So it provides a counterexample to [4, Theorem, p. 17] (in fact, that theorem is correct for $k \geq 3$). Let $m \geq 3$ in Example 4.1 (so $g \geq 1$), choose $G := P_\infty$ and $D := P_1 + P_2$, where $P_1 \neq P_\infty$, $P_2 \neq P_\infty$, and P_1, P_2 lie above different places of $\mathbb{F}_q(x)$. We have

$$C(G, D) = \{(\alpha, \alpha) \mid \alpha \in \mathbb{F}_q\}.$$

This code is evidently self-dual, but $2G - D$ is not canonical. This is trivial for $g \neq 1$; for $g = 1$ it follows from the fact that the canonical divisors are exactly the principal divisors, but $P_1 + P_2 - 2P_\infty$ is not principal according to our assumptions about P_1 and P_2.

Example 4.2 (Codes defined by Kummer extensions of $\mathbb{F}_q(x)$).

In this example we consider the function field $F = \mathbb{F}_q(x, y)$ defined by the equation

$$y^e = f(x)$$

over an arbitrary finite field $\mathbb{F}_q$. We assume

$$f(x) = q_1(x) \cdot \ldots \cdot q_r(x),$$

$$q_i(x) \in \mathbb{F}_q[x] \text{ irreducible, pairwise prime,}$$

$$\deg(q_i(x)) =: m_i, \qquad \deg(f(x)) =: m = m_1 + \cdots + m_r,$$

$$(e, m) = 1, \quad \text{and} \quad q \equiv 1 \bmod e.$$

Observe that every elliptic or hyperelliptic function field over a finite field of characteristic $\neq 2$ which has at least one place of degree 1 is obtained by such an equation (with $e=2$, $m=2g+1$). In $F/\mathbb{F}_q(x)$ exactly the following places are ramified:

the pole of x; we have $(x)_\infty = e \cdot P_\infty$ with $\deg(P_\infty)=1$, the zero of $q_i(x)$ $(i=1,\ldots,r)$; we have $(q_i(x))_0 = e \cdot Q_i$ with a place Q_i of degree m_i.

From this we can determine the divisor of the differential dx and the genus g of F:

$$(dx) = (e-1)\cdot(Q_1+\cdots+Q_r) - (e+1)\cdot P_\infty,$$

$$g = \frac{(e-1)(m-1)}{2}.$$

Let

$$M := \{\alpha \in \mathbb{F}_q \mid f(\alpha) \neq 0, \text{ and there is } \beta \in \mathbb{F}_q \text{ such that } \beta^e = f(\alpha)\}.$$

For $\alpha \in M$ the element $x-\alpha$ has e distinct zeroes in F, and each of the zeroes has degree one. In this way we obtain all places of F of degree one (except P_∞ and the places Q_i with $m_i=1$). As in Example 4.1, we fix a set $U \subseteq M$ with

$$|U| =: s > 0.$$

Let

$$\varphi(x) := \prod_{\alpha \in U} (x-\alpha),$$

$$D := (\varphi(x))_0 =: P_1 + \cdots + P_n \quad \text{with } n = e \cdot s,$$

$$G := r \cdot P_\infty \quad \text{with } r \leq g - 1 + \frac{n}{2}, \quad \text{and} \quad \eta := \frac{dx}{y^{e-1}\cdot\varphi(x)}.$$

It follows that

$$(\eta) = ((m-1)(e-1)-2+n)\cdot P_\infty - D \geq 2r \cdot P_\infty - D = 2G - D,$$

so we can apply Theorem 3.1. It is not difficult to compute the vector $a = (\operatorname{res}_{P_1}\eta, \ldots, \operatorname{res}_{P_n}\eta)$ in this situation: if $\alpha_i := x(P_i)$, $\beta_i := y(P_i)$ then

$$\operatorname{res}_{P_i}(\eta) = \frac{1}{\beta_i^{e-1}\cdot\varphi'(\alpha_i)}.$$

Remark. Similarly to Example 4.2 one can treat the case of the equation

$$y^e = f(x) \in \mathbb{F}_q[x], \quad e \mid \deg(f).$$

This is particularly interesting because the Fermat function field with defining equation

$$y^e + x^e + 1 = 0, \quad (e, q) = 1$$

is of this form. For special values of e these function fields attain the Hasse-Weil bound (cf. [8, p. 83]).

Example 4.3 (Codes defined by Artin-Schreier extensions of $\mathbb{F}_q(x)$).

Now $\mathbb{F}_q$ is an arbitrary finite field,

$$l := \mathrm{char}(\mathbb{F}_q)$$

the characteristic of $\mathbb{F}_q$. The function field F is defined by $F = \mathbb{F}_q(x, y)$ with

$$h(y) = f(x), \quad h(y) \in \mathbb{F}_q[y],\ f(x) \in \mathbb{F}_q[x].$$

Further we assume

(1) $h(y)$ is a separable additive polynomial of degree l^v, i.e.

$$h(y) = \sum_{i=0}^{v} c_i y^{l^i} \quad \text{with } c_i \in \mathbb{F}_q,\ c_0 \neq 0,\ c_v \neq 0.$$

(2) $h(y)$ splits completely into linear factors over $\mathbb{F}_q$, hence the zeroes of $h(y)$ form an additive subgroup of $\mathbb{F}_q$ of order $p := l^v$.

(3) $\deg(f) =: m \not\equiv 0 \bmod q$.

We put together some properties of F [16]:

(4) $(x)_\infty = p \cdot P_\infty$ with a place P_∞ of degree 1, $(\mathrm{d}x) = ((p-1)(m-1)-2) \cdot P_\infty$, and the genus of F is given by $g = \frac{1}{2}(p-1)(m-1)$.

As before we introduce the set

$$M := \{\alpha \in \mathbb{F}_q \mid \text{there is } \beta \in \mathbb{F}_q \text{ with } h(\beta) = f(\alpha)\}.$$

For $\alpha \in M$ the element $x - \alpha$ has p distinct zeroes in F, all of degree one. Except the place P_∞ all places of F of degree one are obtained in this way. Again we fix a set $U \subseteq M$ with $|U| =: s > 0$. Let

$$\varphi(x) := \prod_{\alpha \in U} (x - \alpha),$$

$$D := (\varphi(x))_0 =: P_1 + \cdots + P_n \quad \text{with } n = p \cdot s,$$

$$G := r \cdot P_\infty \quad \text{with } r \leq g - 1 + \frac{n}{2},$$

$$\eta := \frac{\mathrm{d}x}{\varphi(x)}.$$

The divisor of η takes the form

$$(\eta) = (2g-2) \cdot P_\infty - (D - n \cdot P_\infty) = 2\left(g - 1 + \frac{n}{2}\right) \cdot P_\infty - D,$$

hence $2G - D \leq (\eta)$ and we can apply Theorem 3.1. Now it is even easier to compute the vector $a = (\mathrm{res}_{P_1} \eta, \ldots, \mathrm{res}_{P_n} \eta)$. The result is as follows: Let P_i a place in the

support of D. Then there is an $\alpha_i \in U$ with $x(P_i) = \alpha_i$, and we have

$$\mathrm{res}_{P_i}(\eta) = \frac{1}{\varphi'(\alpha_i)} .$$

In the particular case

$$\varphi(x) = c \cdot x + \psi(x^l) \quad \text{with } \psi(T) \in \mathbb{F}_q[T],\ c \neq 0,\ l = \mathrm{char}(\mathbb{F}_q)$$

we have $\varphi'(\alpha_i) = c$ for all $\alpha_i \in U$, and by Theorem 3.1 the code $C(G, D)$ is self-orthogonal (resp. self-dual for $r = g - 1 + \frac{1}{2}n$).

Function fields of the type considered in Example 4.3 often have many places of degree one, so the codes $C(G, D)$ are rather long. We describe a typical case:

Example 4.3.1. Let (in Example 4.3) $q = Q^2$ (Q a prime power) and $F = \mathbb{F}_q(x, y)$ be defined by

$$y^Q + y = x^{Q+1}.$$

F has genus $g = \frac{1}{2}Q(Q-1)$, and for every $\alpha \in \mathbb{F}_q$ the element $x - \alpha$ has Q zeroes of degree one in F (see [7]). One easily checks that the Hasse–Weil bound is attained. Choosing $U := \mathbb{F}_q$ we have (notations as in Example 4.3)

$$\varphi(x) = x^q - x, \qquad \varphi'(x) = -1,$$

$$D = P_1 + \cdots + P_n \quad \text{with } n = q \cdot Q,$$

$$G = r \cdot P_\infty \quad \text{with } r \leq g - 1 + \frac{n}{2} .$$

By Corollary 3.2 the code $C(G, D)$ is a self-orthogonal code of length $q^{3/2}$ over $\mathbb{F}_q$. In case $r = g - 1 + \frac{1}{2}n$ it is a self-dual $[n, \frac{1}{2}n, d]$-code over $\mathbb{F}_q$ with parameters

$$n = q^{3/2} \quad \text{and} \quad d \geq \frac{n}{2} + 1 - g = \frac{1}{2}(q^{3/2} - q + q^{1/2}) + 1.$$

Remark 4.4. In Examples 4.1 and 4.3 the set

$$\{x^i y^j \mid i \geq 0,\ 0 \leq j \leq p-1,\ ip + jm \leq r\}$$

is a basis of $L(r \cdot P_\infty)$ (see [16]). By means of this basis one can easily write down a generating matrix for $C(G, D)$ (with $G = r \cdot P_\infty$ and $D = P_1 + \cdots + P_n$ as in Example 4.3). To this end we define

$$\alpha_v := x(P_v), \qquad \beta_v := y(P_v) \quad (v = 1, \ldots, n),$$

and for all i, j with $0 \leq i$, $0 \leq j \leq p-1$, $ip + jm \leq r$ we define the vector

$$u_{ij} := (\alpha_v^i \beta_v^j)_{v=1,\ldots,n} \in \mathbb{F}_q^n.$$

The matrix E with rows u_{ij} is a generating matrix for the code $C(G, D)$.

In a similar way one can specify a generating matrix in Example 4.2.

Remark 4.5. In many particular cases of our examples the exact minimum distance of $C(G,D)$ can be computed because the modules $L(G)$ are very well known (cf. Remarks 4.4 and 2.2).

References

[1] E. Bombieri, Counting points on curves over finite fields, Sem. Bourbaki, 25e année 1972/73, No. 430.

[2] C. Chevalley, Introduction to the Theory of Algebraic Functions of one Variable (Amer. Math. Soc., New York, 1951).

[3] M. Deuring, Lectures on the Theory of Algebraic Functions of one Variable, Lecture Notes in Mathematics 314 (Springer, Berlin, 1973).

[4] Y. Driencourt and J.F. Michon, Remarques sur les codes géométriques, C.R. Acad. Sci. Paris Sér. I 301 (1) (1985) 15–17.

[5] Y. Driencourt and J.F. Michon, Elliptic codes over fields of characteristic 2, J. Pure Appl. Algebra 45 (1987) 15–39.

[6] Y. Driencourt and J.F. Michon, Quelques propriétés des codes elliptiques sur les corps de caractéristique 2, Preprint, Paris 1985.

[7] A. Garcia and P. Viana, Weierstrass-points on certain non-classical curves. Arch. Math. 46 (1986) 315–322.

[8] V.D. Goppa, Algebraico-geometric codes, Math. USSR-Izv. 21 (1) (1983) 75–91.

[9] H. Hasse, Theorie der relativ zyklischen algebraischen Funktionenkörper, J. Reine Angew. Math. 172 (1934) 37–54.

[10] Y. Ihara; Some remarks on the number of rational points of algebraic curves over finite fields, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (3) (1982) 721–724.

[11] G. Lachaud, Les codes géométriques de Goppa, Sem. Bourbaki, 37e année, 1984/85, No. 641.

[12] J.H. van Lint, Introduction to Coding Theory, Graduate Texts in Mathematics 86 (Springer, Berlin, 1982).

[13] F.J. MacWilliams and N.J.A. Sloane, The theory of error-correcting codes (North-Holland, Amsterdam, 1977).

[14] Y.I. Manin and S.G. Vladut, Linear codes and modular curves, J. Sov. Math. 30 (6) (1985) 2611–2643.

[15] J.F. Michon, Codes de Goppa, Sém. Th. des nombres de Bordeaux, 1983/84, exposé No. 7.

[16] H. Stichtenoth, Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahl-charakteristik, Teil II, Arch. Math. 24 (1973) 615–631.

[17] M.A. Tsfasman, S.G. Vladut and T. Zink, Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachr. 109 (1982) 21–28.